IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of	Group Art Unit: 2135
	Confirmation No. 1080
Kenneth A. Parulski, et al	Examiner: Thomas A. Gyorfi
DIGITAL CAMERA WITH IMAGE AUTHENTICATION	
Serial No. 09/473,522	
Filed 28 December 1999	

Mail Stop APPEAL BRIEF-PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA. 22313-1450

Sir:

APPEAL BRIEF PURSUANT TO 37 C.F.R. 41.37 and 35 U.S.C. 134

Table of Contents

APPELLANTS' BRIEF ON APPEAL

Appellants hereby appeal to the Board of Patent Appeals and Interferences from the rejection of claims 1-25 which was contained in the Office Action mailed July 25, 2007.

A Notice of Appeal is filed concurrently herewith.

In the July 25, 2007 Office Action, the Examiner reopened prosecution responsive to Appellants' previous Appeal Brief. Appellants have chosen to respond to the Office Action by initiating a new appeal.

The fees already paid in conjunction with the previous Notice of Appeal and Appeal Brief should be applied against the fees due for the present Notice of Appeal and Appeal Brief.

Real Party in Interest

The present application is assigned of record to the Eastman Kodak Company. The Eastman Kodak Company is the real party in interest.

Related Appeals and Interferences

No appeals or interferences are known which will directly affect or be directly affected by or have bearing on the Board's decision in the pending appeal.

Status of the Claims

The present application was filed on December 28, 1999 with claims 1-15. New claims 16-25 were subsequently added by amendment. Claims 1-25 are currently pending, with claims 1, 6-10 and 22 being the independent claims. Claims 1-25 stand rejected under 35 U.S.C. §103(a).

Appendix I provides a clean, double spaced copy of the claims on appeal.

Status of Amendments

There have been no amendments filed subsequent to the appealed rejection.

Summary of Claimed Subject Matter

Independent claim 1 is directed to an improvement in a digital camera of the type employing a private key to encrypt a hash of a digital image captured by the digital camera to produce an image authentication signature. The improvement comprises a processor located within the digital camera for generating a random seed entirely from sensor noise within the digital camera and for using the random seed to generate a private key and a public key, and means for storing the private key in a memory in the digital camera for subsequent use in encryption of the hash of the digital image to produce the image authentication signature.

An illustrative embodiment is digital camera 10 shown in FIG. 1. The digital camera 10 includes a processor 18 which creates a public/private key pair, and stores the private key in flash memory 26. See the specification at page 6, lines 12-16, page 8, lines 1-5 and 27-31, page 9, lines 24-25, steps 56 and 58 in FIG. 2, and steps 300 to 340 of FIG. 3. Structure corresponding to the recited means for storing comprises processor 18 operating in conjunction with flash memory 26.

Independent claim 6 is directed to an improvement in a method of producing an image authentication signature in a digital camera employing a private key to encrypt a hash of an image captured by the digital camera. The improvement comprises the steps of generating a random seed entirely from sensor noise in the digital camera and using the random seed to generate a private key in the digital camera, and storing the private key in a memory in the digital camera for subsequent encryption of the hash of the digital image.

An illustrative embodiment of the recited method is shown in steps 56 and 58 of FIG. 2. Steps 300 to 340 of FIG. 3 show a more detailed view of one possible implementation of step 56 of FIG. 2. See the specification at page 6, lines 12-16, page 8, lines 1-5 and 27-31, and page 9, lines 24-25.

Independent claim 7 is directed to a method of authenticating an image captured by a digital camera. The method comprises the steps of generating a random seed entirely from sensor noise in the digital camera and using the random

seed to generate a private key and a public key in the digital camera, storing the private key in a memory in the digital camera, communicating the public key to a user, capturing a digital image, hashing the captured digital image in the digital camera to produce an image hash, encrypting the image hash in the digital camera with the private key to produce a digital signature, and authenticating the digital image by hashing the image outside of the digital camera, decrypting the digital signature using the public key to produce a decrypted signature, and comparing the decrypted signature with the image hash produced outside of the digital camera.

An illustrative embodiment is shown in steps 56 to 78 of FIG. 2. See the specification at page 6, line 5, to page 7, line 9.

Independent claim 8 is directed to a method of manufacturing a digital camera capable of producing a digital signature useful for image authentication, comprising the steps of manufacturing a digital camera with an internal processor for generating a random seed entirely from sensor noise within the digital camera and using the random seed to generate a private key and a public key within the digital camera, storing the public key in a memory in the digital camera and communicating the public key to a camera operator, sending the digital camera to an authentication service, activating the digital camera at the authentication service to produce the private key and public key, registering the public key at the authentication service, and sending the digital camera to a user.

An illustrative embodiment is shown in steps 50 to 58 of FIG. 2. See the specification at page 6, lines 5-8 and 12-16, page 8, lines 1-5, 19-24 and 27-31, and page 9, lines 24-25.

Independent claim 9 is directed to an improvement in a digital camera of the type employing a private key to encrypt a hash of a digital image captured by the digital camera to produce an image authentication signature and a metadata signature corresponding to one or more metadata values. The improvement comprises a processor located within the digital camera for generating a random seed entirely from sensor noise within the digital camera and for using the random seed to generate a private key and a public key, and means for storing the private key in a memory in the digital camera for subsequent use in encryption of the hash

-3-

of the digital image to produce the image authentication signature and the metadata signature.

An illustrative embodiment is digital camera 10 shown in FIG. 1. The digital camera 10 includes a processor 18 which creates a public/private key pair, and stores the private key in flash memory 26. See the specification at page 6, lines 12-16, page 8, lines 1-5 and 27-31, page 9, lines 24-25, page 10, lines 18-31, steps 56 and 58 in FIG. 2, and steps 300 to 340 of FIG. 3. Structure corresponding to the recited means for storing comprises processor 18 operating in conjunction with flash memory 26.

Independent claim 10 is directed to a method of producing an image authentication signature in a digital camera, comprising the steps of capturing a digital image, compressing the captured digital image, generating a random seed entirely from sensor noise in the digital camera and using the random seed to generate a private key and a public key in the digital camera, storing the private key in a memory in the digital camera, providing one or more metadata values, hashing the compressed captured digital image and at least one of the metadata values to produce an image hash, and encrypting the image hash to produce the image authentication signature.

An illustrative embodiment is shown in steps 56 to 68 of FIG. 2. See the specification at page 6, lines 5-28.

Independent claim 22 is directed to an improvement in a digital camera of the type employing a private key to encrypt a digital image captured by the digital camera to produce an image authentication signature. The improvement comprises a processor located within the digital camera for generating the private key from a physically random process entirely based on sensor noise within the digital camera, and means for storing the private key in a memory in the digital camera for subsequent use in encryption of the digital image to produce the image authentication signature.

An illustrative embodiment is digital camera 10 shown in FIG. 1. The digital camera 10 includes a processor 18 which creates a public/private key pair, and stores the private key in flash memory 26. See the specification at page 6, lines 12-16, page 8, lines 1-5 and 27-31, page 9, lines 24-25, steps 56 and 58 in

FIG. 2, and steps 300 to 340 of FIG. 3. Structure corresponding to the recited means for storing comprises processor 18 operating in conjunction with flash memory 26.

Grounds of Rejection to be Reviewed on Appeal

The following issues are presented for review by the Board of Patent Appeals and Interferences:

1. Claims 1, 2 and 4-24 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,889,324 (hereinafter "Kanai") in view of RFC1750 by Eastlake et al. entitled "Randomness Recommendations for Security" (hereinafter "Eastlake").

2. Claims 3 and 25 are rejected under 35 U.S.C. §103(a) as being unpatentable over Kanai in view of Eastlake and in further view of U.S. Patent No. 6,046,768 (hereinafter "Kaneda").

Arguments

1. §103(a) Rejection over Kanai and Eastlake
Claims 1, 4, 5 and 9-15

Appellants initially note that a proper *prima facie* case of obviousness under §103(a) requires that the cited references must teach or suggest all the claim limitations, and that there be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify or combine the reference teachings. See Manual of Patent Examining Procedure (MPEP), Eighth Edition, August 2001, §706.02(j).

Appellants submit that the Examiner has failed to establish a proper *prima facie* case of obviousness in the §103(a) rejection of claims 1-25, in that the proposed combination of references fails to teach or suggest all the limitations of the claims, and in that no cogent motivation has been identified for modifying or combining the reference teachings to reach the claimed invention.

As indicated above, independent claim 1 recites a digital camera having a processor that generates <u>a random seed entirely from sensor noise within the digital camera</u>. The processor is further specified as using the random seed to

generate a private key and a public key. The private key is stored in a memory in the digital camera for subsequent use in encryption of a hash of a digital image to produce an image authentication signature.

In formulating the §103(a) rejection of claim 1, the Examiner characterizes the teachings of the Kanai and Eastlake references in a particular manner. Appellants respectfully disagree with certain aspects of these characterizations, and in addressing the characterizations below may address the references individually. It should be understood that the Appellants are not arguing that the references individually fail to meet the claim limitations, but are instead arguing that the collective teachings of Kanai and Eastlake fail to meet the claim limitations, and actually teach away from those limitations.

Examiner argues that Kanai teaches a processor, located within a digital camera, for generating a random seed, apparently relying on the teachings in column 8, lines 1-7, of Kanai. See the Office Action at page 5, last paragraph. Appellants respectfully disagree. What Kanai teaches in the relied-upon portion is the generation of a random number Nr that is used to authenticate an external IC card as illustrated in FIG. 6 of Kanai. This random number Nr is generated by the digital measurement apparatus and communicated to the IC card, which encrypts the random number Nr using the private key of the manufacturer in order to generate an authentication code. The digital measurement apparatus decrypts the authentication code received from the IC card, using the public key of the manufacturer, to recover a random number Nr'. The IC card is considered successfully authenticated to the digital measurement apparatus if Nr' is equal to the original random number Nr.

It is clear from these teachings of Kanai that the random number explicitly relied upon by the Examiner in formulating the §103(a) rejection is not a random seed of the type that would be used to generate a private key and a public key as recited in claim 1. For example, the random number Nr itself is transmitted to an unauthenticated IC card as indicated in FIG. 6 of Kanai. One skilled in the art would recognize that it would be highly undesirable to transmit to an unauthenticated element in this manner a random seed used to generate private and public keys, as this would severely undermine the security of the system.

Also, a new random number Nr is apparently generated for each instance of authentication carried out by the digital measurement apparatus. It would clearly be undesirable to have to regenerate a new key pair each time the digital measurement apparatus needed to conduct an authentication operation. These facts indicate that the random number Nr in Kanai is not a random seed suitable for use in generating private and public keys. Accordingly, Appellants submit that the Examiner has mischaracterized the Kanai reference in arguing that Kanai teaches the recited processor for generating a random seed.

The Examiner acknowledges that the Kanai reference fails to provide any description regarding the particular manner in which private and public key pairs are generated for the digital measurement apparatus. See the Office Action at page 6, first two lines. Kanai does explicitly state at column 7, lines 29-30, that "it is necessary" that the key pair generation process occur "before" data measurement can be performed by the data measurement apparatus. It is believed that this statement is a direct teaching away from the claimed invention, which utilizes sensor noise generated within the digital camera to generate a random seed that is used to generate a private key and a public key.

Kanai simply does not disclose how or where a random seed could be generated in the described system. As noted above, it is clear that the random number Nr does not constitute such a seed. However, it is stated in column 9, lines 15-18, of Kanai that "actual key-pair generation can be performed when it is determined that the external authentication has been established." Thus, Kanai appears to disclose an arrangement in which performance of key-pair generation within the data measurement apparatus is conditioned on authentication of some external element, such as the IC card. For example, Kanai may contemplate the authenticated external element supplying a random seed to the data measurement apparatus for use therein, which is directly contrary to the limitations at issue calling for a digital camera processor that generates a random seed. Absent such authentication of an external element, it appears that the data measurement apparatus in Kanai may have to rely on key pair generation "performed by the manufacturer of the measurement apparatus in a factory before shipment." See Kanai at column 7, lines 30-33, and column 9, lines 9-10. Again, such disclosure

teaches away from the claimed invention, which advantageously avoids the need for the manufacturer to generate key pairs as well as the need for the digital camera to authenticate external elements before performing key pair generation.

The Examiner argues that the Eastlake reference overcomes the deficiencies of Kanai as applied to claim 1. More specifically, the Examiner characterizes Eastlake as teaching that "one good source of random numbers can be generated entirely from the sensor noise of a digital camera." See the Office Action at page 6, first paragraph. Appellants respectfully disagree. The relied-upon portion of Eastlake, at section 5.3.1, describes an arrangement in which a computer system uses an <u>external video input</u> supplied from a separate camera as a source of random bits for the computer system. There is no teaching or suggestion in Eastlake that the camera referred to therein use <u>its own sensor noise to generate its own random seed</u>. To the contrary, Eastlake simply teaches to supply video from a camera with its lens cap on to a computer system for use <u>in generating a source of random bits in the computer system</u>.

Accordingly, it is believed that the combined teachings of Kanai and Eastlake fail to meet the limitations of independent claim 1. More specifically, the combined teachings fail to teach or suggest the recited processor in a digital camera for generating a random seed entirely from sensor noise within the digital camera and for using the random seed to generate a private key and a public key.

Furthermore, it is believed that insufficient objective evidence of motivation to combine Kanai and Eastlake has been identified by the Examiner. The Examiner in the Office Action at page 6, first paragraph, argues that "[i]t would have been obvious to use sensor noise from the digital camera as the source for the random numbers in the key generation algorithm used by the CPU in the Kenai camera . . . [in order] to use a strong portable source of unpredictable numbers." Appellants respectfully submit that this is a conclusory statement of the sort rejected by both the Federal Circuit and the U.S. Supreme Court. See <u>KSR v. Teleflex</u>, 127 S. Ct. 1727, 1741 (2007), quoting <u>In re Kahn</u>, 441 F. 3d 977, 988 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.").

The statement appears to recite an advantage of the claimed arrangement as alleged motivation for the proposed combination, which is conclusory and therefore improper.

As Appellants noted above, the collective teachings of Kanai and Eastlake fail to teach or suggest a processor in a digital camera that generates a random seed and generates private and public keys from that seed. The Kanai random numbers relied on by the Examiner are clearly not random seeds suitable for use in generating key pairs, and Kanai teaches away from the invention by appearing to require authentication of an external element before key pair generation can proceed. Similarly, the Eastlake reference is silent with regard to generation of a random seed within a digital camera, and appears instead to teach away from the claimed invention by teaching a camera that supplies video to an external computer for further processing in that computer. Accordingly, it is believed that the Examiner has failed to identify sufficient objective motivation for combining Kanai and Eastlake, or for modifying their collective teachings to meet the claimed invention.

Appellants also disagree with the characterization of Eastlake as disclosing a "strong portable source of unpredictable numbers." Eastlake at page 10, section 5, mentions that there "might be" some "hope for strong portable randomness in the future." However, at page 14, Eastlake indicates, with emphasis supplied, that even if a separate computer were to receive a video input from a camera with the lens cap on such data "should not be trusted without some checking in case of hardware failure." The video output from the camera in Eastlake clearly requires further processing in the separate computer in order to generate a source of random bits for that computer. These disclosures in Eastlake represent further teachings away from the claimed arrangement.

Finally, it should be noted that those skilled in the art have had long exposure to the teachings of Eastlake (1994) as well as knowledge of the need for improved cryptographic functionality in digital cameras, and yet none of these skilled artisans, including the Kanai inventors, have heretofore thought to adapt the Eastlake teachings in the manner that the Examiner alleges would have been

obvious. This failure of others to achieve the advantageous arrangements set forth in the present claims constitutes strong evidence of non-obviousness.

It therefore appears that the Examiner in formulating the §103(a) rejection of claim 1 over Kenai and Eastlake has undertaken a piecemeal reconstruction of the claimed invention based upon impermissible hindsight, given the benefit of the disclosure provided by Appellants.

With regard to the Official Notice taken in the Office Action at page 6, last paragraph, to page 7, first paragraph, Appellants respectfully traverse. This Notice is believed to be based on an erroneous interpretation of the disclosure of column 4, lines 10-25, in U.S. Patent No. 5,801,856 (hereinafter "Moghadam"). The relied-upon portion of Moghadam refers to FIG. 2, which shows a light tight enclosure 22 coupled to a computer 24. The text states that the light tight enclosure 22 may be a camera having an onboard computer. It further states that the computer 24 may contain programs for generating encryption keys. There is no teaching or suggestion that the onboard computer contain such programs, as the text clearly states that it is the separate computer 24, and not the light tight enclosure 22, that contains the programs. The Office Notice is therefore believed to be improper, and should be withdrawn.

Independent claims 9 and 10 are believed allowable for reasons similar to those identified above with regard to claim 1.

Dependent claims 4, 5 and 11-15 are believed allowable at least by virtue of their dependence from their respective independent claims.

Claim 2

Dependent claim 2 further recites that the random seed for the private key is produced by processing an image captured from an image sensor of the digital camera so that the random noise level in the captured image is used in producing the random seed. The Kanai reference at column 7, lines 29-30, teaches away from this limitation by stating that "key-pair generating processing" must be done "before performing data measurement." Updates to the key-pair generation in Kanai apparently cannot be performed until "it is determined that the external authentication has been established." See Kanai at column 9, lines 8-21. The

relied-upon portion of the Eastlake reference at page 14, section 5.3.1, first paragraph, teaches that a camera with its lens cap on supplies video to a separate computer and that the video is processed in the separate computer to provide a source of random numbers for the computer. Therefore, the collective teachings of Kanai and Eastlake fail to meet the limitations relating to production of a random seed in a digital camera from the random noise level in an image captured by that camera.

Claim 6

Independent claim 6 calls for generating a random seed entirely from sensor noise in a digital camera and using the random seed to generate a private key in the digital camera. The Examiner again relies on the combination of Kanai and Eastlake. However, as outlined above, the Kanai reference provides no teaching whatsoever regarding the generation of a random seed within a digital camera, and instead suggests that such a seed may be externally supplied since updates to the key-pair generation in Kanai apparently cannot be performed until "it is determined that the external authentication has been established." See Kanai at column 9, lines 8-21. The relied-upon portion of the Eastlake reference at page 14, section 5.3.1, first paragraph, teaches that a camera with its lens cap on supplies video to a separate computer and that the video is processed in the separate computer to provide a source of random numbers for the computer. Accordingly, it is believed that the collective teachings of Kanai and Eastlake fail to meet the limitations of claim 6.

Claim 7

Independent claim 7 calls for generating a random seed entirely from sensor noise in a digital camera and using the random seed to generate a private key and a public key in the digital camera. The Examiner again relies on the combination of Kanai and Eastlake. However, as outlined above, the Kanai reference provides no teaching whatsoever regarding the generation of a random seed within a digital camera, and instead suggests that such a seed may be externally supplied since updates to the key-pair generation in Kanai apparently

cannot be performed until "it is determined that the external authentication has been established." See Kanai at column 9, lines 8-21. The relied-upon portion of the Eastlake reference at page 14, section 5.3.1, first paragraph, teaches that a camera with its lens cap on supplies video to a separate computer and that the video is processed in the separate computer to provide a source of random numbers for the computer. Accordingly, it is believed that the collective teachings of Kanai and Eastlake fail to meet the limitations of claim 7.

Claim 8

Independent claim 8 calls for manufacturing a digital camera with an internal processor for generating a random seed <u>entirely from sensor noise within the digital camera</u> and using the random seed <u>to generate a private key and a public key within the digital camera</u>. The claim also calls for storing the public key in a memory in the digital camera and communicating the public key to a camera operator, sending the digital camera to an authentication service, activating the digital camera at the authentication service to produce the private key and public key, registering the public key at the authentication service, and sending the digital camera to a user.

For the reasons noted above in the context of claim 1, the proposed combination of Kanai and Eastlake fails to teach or suggest a digital camera with an internal processor for generating a random seed entirely from sensor noise within the digital camera.

In addition, the Examiner argues that the limitation relating to sending the digital camera to an authentication service is shown in column 7, lines 29-33, of Kanai. However, this portion of the Kanai reference refers to key-pair generation performed by a manufacturer in a factory before shipment. There is no mention in the relied-upon portion of Kenai of sending the measurement apparatus anywhere, while the claim includes separate steps of manufacturing the digital camera and sending the digital camera to an authentication service that performs activation and registers the public key.

Accordingly, it is believed that the proposed combination of Kanai and Eastlake fails to meet each and every limitation of claim 8.

-12-

Claims 16-21

Each of these claims specifies that an algorithm stored in firmware memory is used to produce a private key, and further that the algorithm is deleted from firmware memory after the private key is generated. The Examiner argues that this limitation is met by Kanai, but Kanai fails to disclose at least the deletion of an algorithm from firmware memory after that algorithm is used to generate a private key. Although Kenai in column 9, lines 8-21, refers to the possibility that a new key generating algorithm may be used, it does not disclose that an algorithm used to generate a private key is necessarily deleted after that private key is generated. Accordingly, the combined teachings of Kanai and Eastlake fail to meet the limitations in question.

Claim 22

Independent claim 22 calls for a digital camera comprising a processor located within the digital camera for generating a private key from a physically random process <u>entirely based on sensor noise within the digital camera</u>. The Examiner again relies on the combination of Kanai and Eastlake. However, as outlined above, Kanai fails to provide any disclosure regarding generation of a private key from a physically random process. The random numbers referred to in Kanai are communicated to unauthenticated external elements, such as an IC card, as part of an authentication process, and are thus not suitable for use in generating private keys. Eastlake teaches to supply video output from a camera with its lens cap on to a separate computer for further processing in that computer. Thus, the collective teachings of Kanai and Eastlake fail to meet the limitations at issue.

Claim 23

Dependent claim 23 further recites that the physically random process used to generate the private key is dependent upon a random seed produced from <u>a</u> <u>random noise level in a captured image</u>. The Kanai reference at column 7, lines 29-30, teaches away from this limitation by stating that "key-pair generating processing" must be done "before performing data measurement." Updates to the

key-pair generation in Kanai apparently cannot be performed until "it is determined that the external authentication has been established." See Kanai at column 9, lines 8-21. The relied-upon portion of the Eastlake reference at page 14, section 5.3.1, first paragraph, teaches that a camera with its lens cap on supplies video to a separate computer and that the video is processed in the separate computer to provide a source of random numbers for the computer. Therefore, the collective teachings of Kanai and Eastlake fail to meet the limitations relating to <u>production of a random seed in a digital camera from the random noise level in an image captured by that camera</u>. Accordingly, it is believed that the limitations of claim 23 are not obvious in view of Kanai and Eastlake.

Claim 24

Dependent claim 24 recites that the random noise level used to produce the random seed is produced by random dark field image data taken from the image sensor. The Examiner relies primarily on Eastlake. However, the relied-upon portion of that reference teaches that input from a "camera with the lens cap on" is supplied to an external computer for further processing and that without additional external operations the random noise from the camera "<u>should not be trusted</u>." This is a direct teaching away from the limitations in question. Accordingly, it is believed that the limitations of claim 24 are not obvious in view of Kanai and Eastlake.

2. §103(a) Rejection over Kanai, Eastlake and Kaneda
Claim 3

Dependent claim 3 recites that the processor causes a variable gain amplifier to be <u>in a high gain condition</u> when an initial test image is captured, where a random noise level in the captured image is used to produce a random seed. The Examiner argues that these limitations are met by the combination of Kanai, Eastlake and Kaneda. However, as noted above, the Kanai reference at column 7, lines 29-30, teaches away from this limitation by stating that "key-pair generating processing" must be done "before performing data measurement."

This apparently means that a key pair must be generated before any images are captured by the data measurement apparatus in Kanai. Moreover, Kanai fails to teach or suggest the production of a random seed in a digital camera, and Eastlake fails to supplement this fundamental deficiency of Kanai. The Examiner seems to argue that the recited variable gain amplifier is met by amplifier AMP3 in FIG. 34 of Kaneda. However, this variable gain amplifier is used to amplify a hand vibration angle displacement signal as detected by a blur detection sensor SA. See Kaneda at column 19, lines 42-44. The amplifier AMP3 is not described as being controlled into a high gain condition when an initial test image is captured, as required by the limitations at issue. Moreover, it is believed that one skilled in the art would not be motivated to look to amplifiers specifically used to amplify a hand vibration angle detection signal for teachings relating to amplification of captured test images. Accordingly, it is believed that the proposed combination of Kanai, Eastlake and Kaneda fails to meet the particular limitations of dependent claim 3, and further that there is insufficient motivation for the proposed combination.

Claim 25

Dependent claim 25 recites that the processor causes a variable gain amplifier to be <u>in a high gain condition</u> when random dark field image data is captured, where the random dark field image data is used to generate a private key in a digital camera. The Examiner argues that these limitations are met by the combination of Kanai, Eastlake and Kaneda. However, as noted above, the Kanai reference at column 7, lines 29-30, teaches away from this limitation by stating that "key-pair generating processing" must be done "before performing data measurement." This apparently means that a key pair must be generated before any images are captured by the data measurement apparatus in Kanai. Moreover, Kanai fails to teach or suggest the production of a random seed in a digital camera, and Eastlake fails to supplement this fundamental deficiency of Kanai. The Examiner seems to argue that the recited variable gain amplifier is met by amplifier AMP3 in FIG. 34 of Kaneda. However, this variable gain amplifier is used to amplify a hand vibration angle displacement signal as detected by a blur
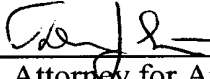
detection sensor SA. See Kaneda at column 19, lines 42-44. The amplifier AMP3 is not described as being controlled into a high gain condition when an initial test image is captured, as required by the limitations at issue. Moreover, it is believed that one skilled in the art would not be motivated to look to amplifiers specifically used to amplify a hand vibration angle detection signal for teachings relating to amplification of captured test images. Accordingly, it is believed that the proposed combination of Kanai, Eastlake and Kaneda fails to meet the particular limitations of dependent claim 25, and further that there is insufficient motivation for the proposed combination.

Conclusion

For the above reasons, Appellants respectfully request that the Board of Patent Appeals and Interferences reverse the rejection by the Examiner and mandate the allowance of claims 1-25.

Respectfully submitted,

Thomas J. Strouse/phw   Attorney for Appellants
Telephone: 585-588-2728   Registration No. 53,950
Facsimile: 585-477-4646
Enclosures
If the Examiner is unable to reach the Appellants' Attorney at the telephone number provided, the Examiner is requested to communicate with Eastman Kodak Company Patent Operations at (585) 477-4656.

Appendix I - Claims on Appeal

1.   In a digital camera of the type employing a private key to encrypt a hash of a digital image captured by the digital camera to produce an image authentication signature, the improvement comprising:

(a)   a processor located within the digital camera for generating a random seed entirely from sensor noise within the digital camera and for using the random seed to generate a private key and a public key; and

(b)   means for storing the private key in a memory in the digital camera for subsequent use in encryption of the hash of the digital image to produce the image authentication signature.

2.   The digital camera claimed in claim 1, further including an image sensor for capturing images, and wherein the processor includes means for producing a random seed for the private key by processing an image captured from the image sensor so that the random noise level in the captured image is used in producing the random seed.

3.   The digital camera according to claim 2, further including:

(i)   a variable gain amplifier coupled to the image sensor;

(ii)   an analog-to-digital converter coupled to the variable gain amplifier and the processor for producing digital signals corresponding to the captured images; and

(iii)   the processor causing the variable gain amplifier to be in a high gain condition when the initial test image is captured.

4.   The digital camera claimed in claim 1, wherein the processor includes one or more algorithms for producing the random seed, wherein the random seed is used to produce a random number k, and for using the random number k to create the image authentication signature by hashing the raw image data prior to image processing.

5.   The digital camera claimed in claim 4, wherein the processor includes an image processing algorithm which uses JPEG compression.

6.   In a method of producing an image authentication signature in a digital camera employing a private key to encrypt a hash of an image captured by the digital camera, the improvement comprising the steps of:

(a)   generating a random seed entirely from sensor noise in the digital camera and using the random seed to generate a private key in the digital camera; and

(b)   storing the private key in a memory in the digital camera for subsequent encryption of the hash of the digital image.

7.   A method of authenticating an image captured by a digital camera, comprising the steps of:

(a)   generating a random seed entirely from sensor noise in the digital camera and using the random seed to generate a private key and a public key in the digital camera;

(b)   storing the private key in a memory in the digital camera;

(c)   communicating the public key to a user;

(d)   capturing a digital image;

(e)   hashing the captured digital image in the digital camera to produce an image hash;

(f)   encrypting the image hash in the digital camera with the private key to produce a digital signature; and

(g)   authenticating the digital image by hashing the image outside of the digital camera, decrypting the digital signature using the public key to produce a decrypted signature, and comparing the decrypted signature with the image hash produced outside of the digital camera.

8.   A method of manufacturing a digital camera capable of producing a digital signature useful for image authentication, comprising the steps of:

(a)   manufacturing a digital camera with an internal processor for generating a random seed entirely from sensor noise within the digital camera and using the random seed to generate a private key and a public key within the digital camera, storing the public key in a memory in the digital camera and communicating the public key to a camera operator;

(b)   sending the digital camera to an authentication service;

(c)   activating the digital camera at the authentication service to produce the private key and public key, and registering the public key at the authentication service; and

(d)   sending the digital camera to a user.

9.   In a digital camera of the type employing a private key to encrypt a hash of a digital image captured by the digital camera to produce an image authentication signature and a metadata signature corresponding to one or more metadata values, the improvement comprising:

(a)   a processor located within the digital camera for generating a random seed entirely from sensor noise within the digital camera and for using the random seed to generate a private key and a public key; and

(b)   means for storing the private key in a memory in the digital camera for subsequent use in encryption of the hash of the digital image to produce the image authentication signature and the metadata signature.

10.   A method of producing an image authentication signature in a digital camera, comprising the steps of:

(a)   capturing a digital image;

(b)   compressing the captured digital image;

(c)   generating a random seed entirely from sensor noise in the digital camera and using the random seed to generate a private key and a public key in the digital camera;

(d)   storing the private key in a memory in the digital camera;

(e)   providing one or more metadata values;

(f)   hashing the compressed captured digital image and at least one of the metadata values to produce an image hash; and

(g)   encrypting the image hash to produce the image authentication signature.

11.   The method according to claim 10 further including the step of storing in an image file in the digital camera, the image authentication signature, the compressed digital image data, and the one or more metadata values.

12.   The method according to claim 10 wherein the encrypting step includes encrypting the image hash with a private key produced in the digital camera to produce the image authentication signature.

13.   The method according to claim 10 wherein the encrypting step includes encrypting the image hash with the private key to produce the image authentication signature; and further including the step of:

authenticating the captured digital image by hashing the compressed digital image outside of the digital camera, decrypting the image authentication signature using the public key to produce a decrypted signature, and comparing the decrypted signature with the image hash produced outside of the digital camera.

14.   The method according to claim 10 further including the steps of: hashing the uncompressed captured digital image to produce a random number k; and wherein the encrypting step includes using the random number k to produce the image authentication signature.

15.   The method according to claim 10 wherein the encrypting step further produces a metadata signature corresponding to the one or more metadata values.

16.   The digital camera according to claim 1, further including firmware memory, wherein the private key is produced using an algorithm stored in the firmware memory and wherein the algorithm is deleted from the firmware memory after the private key is generated.

17.   The method according to claim 6, wherein the private key is produced using an algorithm stored in firmware memory in the digital camera, and wherein the algorithm is deleted from the firmware memory after the private key is generated.

18.   The method according to claim 7, wherein the private key is produced using an algorithm stored in firmware memory in the digital camera, and wherein the algorithm is deleted from the firmware memory after the private key is generated.

19.   The method according to claim 8, wherein the private key is produced using an algorithm stored in firmware memory in the digital camera, and wherein the algorithm is deleted from the firmware memory after the private key is generated.

20.   The digital camera according to claim 9, further including firmware memory, wherein the private key is produced using an algorithm stored in the firmware memory and wherein the algorithm is deleted from the firmware memory after the private key is generated.

21.   The method according to claim 10, wherein the private key is produced using an algorithm stored in firmware memory in the digital camera, and wherein the algorithm is deleted from the firmware memory after the private key is generated.

22.   In a digital camera of the type employing a private key to encrypt a digital image captured by the digital camera to produce an image authentication signature, the improvement comprising:

(a)   a processor located within the digital camera for generating the private key from a physically random process entirely based on sensor noise within the digital camera; and

(b)   means for storing the private key in a memory in the digital camera for subsequent use in encryption of the digital image to produce the image authentication signature.

23.   The digital camera claimed in claim 22, further including an image sensor for capturing images, and wherein the physically random process is dependent upon a random seed produced from a random noise level in a captured image.

24.   The digital camera claimed in claim 23 wherein the random noise level is produced by random dark field image data taken from the sensor.

25.   The digital camera according to claim 24, further including:

(i)   a variable gain amplifier coupled to the image sensor;

(ii)   an analog-to-digital converter coupled to the variable gain amplifier and the processor for producing digital signals corresponding to the captured images; and

(iii)   the processor causing the variable gain amplifier to be in a high gain condition when the random dark field image data is captured.

<u>Appendix II - Evidence</u>

None

Appendix III – Related Proceedings

None